Performance Work Statement (PWS)
Enterprise Network Cyber Defense
08 November 2018

1.0 INTRODUCTION

The Government is acquiring technical engineering and program management services to support carrying out a technical subset of the doctrinal DOD Cyber Security Service Provider (CSSP) functions. These functions include the protection from, detection of and response to cyberspace attacks. The scope of the functions and services has increased from previously contracted support. The Enterprise Network currently includes approximately 9000 SIPRNet hosts and approximately 110,000 NIPRNet Hosts. There are 85+ sites connected to the NIPRNet portion of the Enterprise Network and 35 sites with SIPRNet connectivity. There are total of 200+ network sensors within the Enterprise Network sensor grid. Additionally, 20-30 Web Application Firewalls (WAF) are implemented in key locations across the Enterprise Network. The Government's goal is to disrupt, deny and degrade network adversaries' ability to influence the confidentiality, integrity, availability, authentication and non-repudiation of IT services provided to users on joint networks.

2. BACKGROUND

The Government has an operational and staff organization supporting global Enterprise Network Command and Control (C2) capabilities for forces stationed around the world including forces within the Joint Information Environment (JIE). The Government executes defensive cyber operations – internal defensive measures (DCO-IDM) within the global Enterprise Network and joint networks to include protection, detection, response, recovery, and sustainment functions in alignment with the DOD Instruction 8530.01, which serves as the CSSP program's governing directive.

The Defensive Cyber Operations Section (DCOS) is responsible for technical CSSP functions, as well as DCO-IDM missions. DCOS duties encompass the full range of Computer Network Defense (CND) functions from incident handling to malware analysis and sensor signature management. DCOS facilitates 24 by 7 centralized command and control (C2) of CND personnel and assets to achieve speed of action and uniformity of controls. Additionally, DCOS directly oversees the application of information assurance (IA) controls and enterprise CND services for all out-sourced information technology (IT) vendors supporting Government systems and enclaves per DOD Instruction 8500.01.

3. SCOPE

The scope supports DCOS by analyzing network traffic, identifying malicious and unauthorized activity, and responding to intrusion incidents; implementing, configuring, operating, and maintaining network defense systems; and auditing network security controls, managing enterprise vulnerabilities, drafting formal direction for review and ensuring compliance with enterprise remediation measures. The scope also includes operations of the DCOS internal workforce training program and maintaining a workforce consistent with DOD IA workforce standards, per the DOD Manual 8570.01-M. The primary location of work is Quantico, VA, with secondary sites in San Diego, CA and Kansas City, MO. It is estimated that approximately 90% of effort will be performed at the primary location and the remaining 10% will be performed in San Diego, CA. It is expected that the effort required in San Diego, CA will be relocated to Kansas City, MO during the first 24 months of the task order period of performance. Additional travel may be required.

Top Secret/SCI (TS/SCI) access is required for contractor personnel to perform tasks 5.2 (Discovery and Counter Infiltration), 5.5.2 (Mitigation Action), and 5.5.3 (Information Assurance Red Team) per this PWS. TS/SCI clearances are required in order to have access to the Government work spaces, creation and receipt of JWICS accounts, and access to threat reports related to Cyber Security. Secret access is required for all other contractor personnel per this PWS. Secret clearances are required in order to have access to the government work spaces, creation and receipt of SIPRNet accounts, and access to secret threat reports related to Cyber Security.

4. APPLICABLE DIRECTIVES/DOCUMENTS

The contractor shall adhere to the following documents (as revised) in accordance with paragraph 5.0, Performance Requirements:			
Document	No./Version	Title	Date
DODI	8500.01	Cybersecurity	03/14/2014
DoDD	8140.01	Cyberspace Workforce Management	08/11/2015
DODI	8530.01	Cybersecurity Activities Support to DOD Information Network Operations	07/25/2017
DOD Manual	8570.01-M	Information Assurance Workforce Improvement Program	11/10/2015
DOD Manual	8530.01-M	Computer Network Defense Service Provider Certification And Accreditation Process	12/17/2003
CJCSM	6510.01B	Cyber Incident Handling Program	07/10/2012
CJCSM	6510.03	Department Of Defense Cyber Red Team Certification And Accreditation	02/28/2013
SECNAVINST	5239.19	Department of the Navy Computer Network Incident Response and Reporting Requirements	03/18/2008
NIST	V1.0	NIST Cybersecurity Framework	2/12/2014
NIST	800-115	Technical Guide to Information Security Testing and Assessment	9/2008
MCWP	5-10	Marine Corps Planning Process	05/02/2016

5. PERFORMANCE REQUIRMENTS

The contractor shall provide support services in the work areas listed below.

5.1. Program Management

The Contractor shall provide program management support under this task order (TO). This includes the management and oversight of all activities performed by contractor personnel, including subcontractors, to satisfy the requirements identified in this PWS. The Contractor shall identify a Program Manager (PM), by name, whom shall provide onsite management, direction, administration, quality control, and leadership of the execution of this TO. The Contractor shall perform all activities necessary to ensure the accomplishment of timely and effective support by implementing productivity and management methods ("timely" and "effective" means the activities meet the minimum mandatory requirements identified in CJCSM 6510.01B, “Cyber Incident Handling Program,” dated 10 Jul 2012 or later, and SECNAVINST 5239.19 “Department of the Navy Computer Network Incident Response and Reporting Requirements”, dated 18 Mar 2008 or later.

5.1.1. Coordinate a Project Kick-Off Meeting

The Contractor shall schedule and coordinate a Project Kick-Off Meeting at a Government –approved location. The meeting will provide an introduction between the Contractor personnel and Government personnel who will be involved with this scope. The meeting will provide the opportunity to discuss transition, technical, management, and security issues, and travel authorization and reporting procedures. At a minimum, the attendees shall include the Contractor’s Key Personnel, Government representatives and directorates, other relevant Government personnel,

and the contracting officer's representative (COR). The Contractor shall provide the following at the Kick-Off meeting:

a. Brief Status of Transition Activities
b. Quality Control Plan (QCP) – (CDRL A002)

5.1.2. Monthly Status Reports (MSRs) (CDRL A001)

The Contractor shall develop and provide an MSR using Microsoft (MS) Office Suite applications, by the twelfth (12^{th}) of each month via electronic mail to the Technical Point of Contact (TPOC) and the COR.

5.1.3. Convene Technical Status Meetings (CDRL A003)

The Contractor PM shall convene a monthly Technical Status Meeting with the TPOC, COR, and other Government stakeholders. The purpose of this meeting is to ensure all stakeholders are informed of the monthly activities and MSR, provide opportunities to identify other activities and establish priorities, and coordinate resolution of identified problems or opportunities. The Contractor PM shall provide minutes of these meetings, including attendance, issues discussed, decisions made, and action items assigned, to the COR within five workdays following the meeting.

5.1.4. Project Management Plan (PMP) (CDRL A002)

The Contractor shall document all support requirements in a PMP.

The PMP shall:

a. Describe the proposed management approach
b. Contain detailed Standard Operating Procedures (SOPs) for all tasks
c. Include milestones, tasks, and subtasks required in this TO
d. Provide for an overall Work Breakdown Structure (WBS) and associated responsibilities and partnerships between or among Government organizations
e. Include the Contractor's Quality Control Plan (QCP)
f. Include the Contractor's Communication Management Plan (CMP)
g. Include the Contractor's Risk Management Plan (RMP)
h. Include the Contractor's Integrated Master Schedule (IMS)

The Contractor shall provide the Government with a draft PMP, on which the Government will make comments. The final PMP shall incorporate the Government's comments.

The PMP is an evolutionary document that shall be updated annually at a minimum. The Contractor shall work from the latest Government-approved version of the PMP.

5.1.5. Trip After Action Reports (CDRL A002)

The Government will identify the need for a Trip Report when the request for travel is submitted. The Contractor shall keep a summary of all long-distance travel including, but not limited to, the name of the employee, location of travel, duration of trip, and point of contact (POC) at travel location. All trips made by the Contractor on behalf of the program require an After Action Report (AAR) to be submitted 7 business days from the date of return.

5.1.6. Quality Control Plan (CDRL A002)

The Contractor shall provide a draft Quality Control Plan (QCP) 30 days after contract award and a final QCP 30 days after initial Government review. The Contractor shall periodically update the QCP as changes in program processes are identified.

5.1.7. Transition-In Plan (CDRL A002)

All transition activities will be completed 60 calendar days after the start date of the order. The Contractor shall

ensure that there will be minimum service disruption to vital Government business and no service degradation during the 60-day transition period. The Contractor shall deliver an updated Transition-In Plan within five workdays of task order start.

5.1.8. Transition-Out Plan (CDRL A002)

The Transition-Out Plan shall facilitate the accomplishment of a seamless transition from the incumbent to an incoming contractor/Government personnel at the expiration of the TO. The Contractor shall provide a Transition-Out Plan not later than 90 calendar days prior to expiration of the TO. The Contractor shall identify how it will coordinate with the incoming contractor and/or Government personnel to transfer knowledge regarding the following:

a. Project management processes
b. Points of contact
c. Location of technical and project management documentation
d. Status of ongoing technical initiatives
e. Appropriate contractor–to-contractor coordination to ensure a seamless transition.
f. Schedules and milestones
g. Actions required of the Government.

The Contractor shall also establish and maintain effective communication with the incoming contractor/Government personnel for the period of the transition via weekly status meetings.

5.2. Discovery and Counter-Infiltration (D&CI)

The Contractor shall provide support in Incident Management, Hunt, and Cyber Threat Analysis Cell (CTAC) to defend the Enterprise Network. This tasking will support the detection and response to all malicious activity throughout the Enterprise Network to include classified environments.

5.2.1. Incident Management (IM)

5.2.1.1. Incident Response Support

The Contractor shall provide 24 x 7 x 365 support to conduct real-time analysis of ongoing IA / CND events on the Enterprise Network, identifying incidents and making recommendations to protect the Enterprise Network. The Contractor shall lead efforts in collecting and analyzing network and computing events presented via numerous sources in order to identify and document malicious or unauthorized activity on the Enterprise Network. The Contractor shall conduct advanced data analysis using data science techniques to identify malicious activity not detected by existing signatures. The Contractor shall conduct constant tuning of signatures and alerts to maximize the detection of malicious activity. The Contractor shall conduct initial, formal incident reporting (outlined in CJCSM 6510.01B, “Cyber Incident Handling Program,” dated 10 Jul 2012 or later) and documenting technical details in a Database. The Contractor shall appropriately resolve daily incidents tracked in the database. The Contractor shall use appropriate skills and techniques in scoping, containing and eradicating incidents based on the processes outlined in CJCSM 6510.01B, “Cyber Incident Handling Program,” dated 10 July 2012 or later. Additionally, the Contractor shall be responsible for supporting the transition of network defense configurations as informed by resolved incidents in order to prevent future occurrences. The Contractor shall be responsible for continuity of services as data sources, analysis tools, and techniques will evolve to changes in the government technical computing environment as well as by mandates from parent organizations. These efforts will support the analysis and correlation of over 1 billion events per day (on average). During calendar year 2016, this resulted in 3,665 incidents detected and handled within the Enterprise Network. On average, each incident lasted 15 days. The Contractor shall perform 24x7x365 support from the primary site in Quantico, VA. Additional on-site support is required at the secondary location in San Diego, CA.

The Contractor shall:

a. Maintain the body of documentation that describes DCOS Computer Network Defense (CND) Watch Support and Incident Response tactics, techniques and procedures.

b. Receive and analyze network alerts to determine the cause of those alerts.
c. Receive and analyze reports from multiple sources to determine possible causes of such alerts and tune DCOS detection capabilities to alert on future occurrences
d. Monitor external data sources to maintain visibility of net defense threat conditions and emerging threats to the Enterprise Network and determine enterprise exposure to recommend preemptive defensive measures. (CDRL A002)
e. Inspect, identify and analyze network traffic for possible malicious and anomalous network activity.
f. Utilize data science techniques (Data Preprocessing, Data Transformation, Descriptive Statistical Analysis, Centrality Analysis, Connected Components Analysis, Mutual Information Analysis, Clique Tree Analysis, etc) to identify malicious activity not identified by deployed signatures.
g. Create a minimum of 330 incident records per month maintaining an overall monthly rejection rate for draft incident records at or below 20% and an overall draft promotion rate at or above 85%.
h. Maintain 65% of normal staffing levels (as defined by the contractor) at all times.
i. Coordinate with DCOS staff and outsourced IT-based process vendor personnel to investigate and validate network alerts. Coordinate with DCOS staff and outsourced IT-based process vendor personnel to investigate and validate network alerts.
j. Analyze log files from a variety of sources within the Enterprise Network to characterize anomalous activity. (CDRL A002)
k. Conduct initial troubleshooting of network sensor availability and coordinate with DCOS Sensor Grid Support technicians to maintain sensor availability.
l. Request refinements to user-defined signatures for network sensors to enhance overall effectiveness of the Enterprise Network sensor grid. Track and validate refinement requests and provide metrics on these activities monthly. (CDRL A002)
m. Request refinements to event correlation rules for implementation on the Enterprise Network security information and event manager (SIEM). Track and validate refinement requests and provide metrics on these activities monthly. (CDRL A002)
n. Develop methods for automating incident detection. Provide quarterly reports on new automation actions and their results. Document the technical details of suspected network incidents utilizing internal reporting database to support incident response and reporting requirements (CDRL A002).
o. Perform event correlation using information gathered from multiple sources within the Enterprise Network to gain situational awareness and determine the impact of a network attack.
p. Notify DCOS Managers and appropriate parties of critical network incidents articulating the event's history, status, and potential impact. (CDRL A002)
q. Support post-mortem analysis of the magnetic and optical media collected from compromised systems.
r. Collect and analyze network intrusion artifacts from a variety of sources to include logs, system images and packet captures to enable mitigation of network incidents within the Enterprise Network.
s. Perform initial collection of system images, in a forensic sound manner, to develop mitigation and remediation actions on the Enterprise Network. (CDRL A002)
t. Coordinate with and provide expert technical support to USMC Information Assurance managers, on-site technicians and outsourced IT-based process vendor technicians during incidents to restore integrity to the Enterprise Network.
u. Coordinate with intelligence analysts to correlate threat assessment data with operational reporting through sensor grid and multiple sources within the Enterprise Network.
v. Document and report incidents within the MCD from initial detection through final resolution using standard DOD incident reporting methods (refer to CJCSM 6510.01B, "Cyber Incident Handling Program," dated 10 Jul 2012 or later). (CDRL A002)
w. Perform incident triage to determine scope, urgency, and potential operational impact by identifying the specific vulnerability and making recommendations which enable rapid remediation at the enterprise level.
x. Serve as technical experts and liaisons to external incident response personnel and brief incident details as necessary.
y. Provide remote incident handling support such as forensics collections, intrusion correlation tracking, threat analysis and direct system remediation tasks to on-site personnel.
z. Develop and publish incident response guidance and high-quality incident reports to appropriate audiences. (CDRL A002)
aa. Upon resolution of network incidents, create custom signatures or correlation rules to detect future incidents as well as make Enterprise Network protection recommendations to enhance passive resistance to

future attack. Validate the effectiveness of any signatures or correlation rules created.

bb. Maintain the deployable CND toolkit and stand prepared to support the DCOS fly-away team to conduct onsite support (approximately once every six months) to respond to critical CND incidents in accordance with SECNAVINST 5239.19 “Department of the Navy Computer Network Incident Response and Reporting Requirements”, dated 18 Mar 2008 or later.

cc. Provide support required to maintain the Government’s CSSP accreditation per the standards set forth in the CSSP program manual, DOD -8530.01-M, (dated 17 Dec 03 or later) to include documentation and technical writing support as needed.

5.2.1.2. Advanced Incident Response Support and Quality Assurance

The Contractor shall provide 24 x 7 x 365 support and is responsible for the technical execution of incident handling functions as well as directly responding to severe network incidents. The Contractor shall deploy various techniques to discover and resolve evidence of malicious activity and open vulnerabilities on the Enterprise Network. Technical execution shall align with CJCSM 6510.01B, "Cyber Incident Handling Program," dated 10 Jul 2012 or later, or superseding directive. The Contractor shall be responsible for continuity of services as data sources, analysis tools, and techniques evolve to changes in the Government's technical computing environment as well as by mandates from parent organizations.

The Contractor shall:

a. Maintain the body of documentation that describes DCOS CND Advanced Incident Response tactics, techniques and procedures (CDRL A002).

b. Support the implementation of the latest CND policies, regulations, and compliance documents specifically related to network protections policies of the USMC, Department of the Navy (DON) and DoD.

c. Prepare detailed recommendations for network defense improvements to close or mitigate incidents on the Enterprise Network. (CDRL A002)

d. Review and validate incidents tracked on the MCD.

e. Provide incident reports, summaries, and other situational awareness information as required. (CDRL A002)

f. Directly manage severe network incidents (e.g., coordinate documentation, work efforts, resource utilization within the organization) from inception to final after action reporting.

g. Conduct event trend analysis to identify breaches of the Enterprise Network and coordinate with DCOS Incident Response to resolve compromises of the network.

h. Review incident reporting and intelligence products from adjacent and higher DoD CSSP organizations and cyber defense operational reporting to develop new methods of identifying attacks against the Enterprise Network.

i. Make requests to the DCOS Sensor Grid Support Section to enhance network defense configurations on a daily basis. Provide monthly metrics regarding the number and nature these requests. (CDRL A002)

j. Coordinate with certification and accreditation authorities, network managers, and system administrators and IA managers to correct policy infractions.

k. Make recommendations concerning the overall improvement of network security posture through changes in IT service provisioning on a weekly basis (CDRL A002).

l. Interface with external organizations (e.g., public affairs, law enforcement, Command or Component Inspector General) to ensure appropriate and accurate dissemination of incident and other CND information.

m. Request enterprise protection measures based on incident trends. Provide monthly metrics regarding the number and nature these requests. (CDRL A002)

n. Maintain a deployable CND toolkit and stand prepared to lead the DCOS fly-away team in conducting onsite support (approximately once every six months) during critical incidents as required per SECNAVINST 5239.19 "Department of the Navy Computer Network Incident Response and Reporting Requirements," dated 18 Mar 2008 or later.

o. Provide support required to maintain the Government's CSSP accreditation per the standards set forth in the CSSP program manual, DoD O-8530.1-M, (dated 17 Dec 03 or later) to include documentation and technical writing support as needed.

5.2.2. Hunt Team

The DCOS Hunt Team is responsible for defensive cyber counter-infiltration operations against Advanced Persistent Threats (APT) within the Enterprise Network. The Contractor shall be responsible for operations and sustainment functions to DCOS Hunt Team operations to include Server/Host, Network, and Planning. On average, 10 operations are executed per year at a length of 4-6 weeks each.

The Contractor shall:

a. Maintain the body of documentation that describes the tactics, techniques and procedures that comprise the Hunt team (CDRL A002).
b. Assess and identify Advanced Persistent Threat (APT) activities within an Operating System (OS). (CDRL A002)
c. Develop and document tactics, techniques, and procedures (TTPs) for resource planning, operations, and analysis. (CDRL A002)
d. Research, identify, and verify new APT TTPs to strengthen the overall security posture of the Enterprise Network. (CDRL A002)
e. Conduct Hunt planning utilizing the Government's Planning Process, per the standards set forth in policy to be provided at time of award, to include documentation and planning support as needed.
f. Coordinate with intelligence analysts and external threat intelligence reporting sources to support maintenance of current APT TTPs.
g. Directly manage Hunt operations (e.g., coordinate documentation, work efforts, resource utilization within the organization) from inception to final after action reporting by leading the technical efforts of the Hunt Team.

5.2.3. Cyber Threat Analysis Cell (CTAC)

The Contractor is responsible for providing support to the CTAC, which serves as the principle supporting entity to all tailored incident response operations. This analytical cell, which consists of the malware and forensic analysis and exploit analysis teams, executes all advanced analysis for Government defensive cyber operations.

5.2.3.1. Malware and Forensics Support

The Contractor is responsible for responding to incidents using appropriate techniques in Surface Analysis, Runtime Analysis, and Static Analysis. The Contractor shall adhere to the procedures outlined in CJCSM 6510.01B, "Cyber Incident Handling Program," dated 10 Jul 2012 or later for disk/drive image dissection processes. Additionally, the Contractor shall support the transition of network defense configurations as informed by resolved incidents in order to prevent future occurrences. The Contractor is responsible for maintaining currency as data sources, analysis tools, and techniques evolve to changes in the technical computing environment as well as by mandates from parent organizations. During calendar year 2016, the Government team completed over 597 forensic investigations and analyzed over 660 malicious files.

The Contractor shall:

a. Maintain the body of documentation that describes DCOS CND Incident Response tactics, techniques and procedures, to include an emphasis on Malware and Forensic Analysis (CDRL A002).
b. Support post-mortem analysis of the magnetic and optical media collected from compromised systems. (CDRL A002)
c. Perform initial, forensically sound collection of system images and inspect same to discern possible mitigation and remediation of network incidents on the Enterprise Network.
d. Perform remote incident handling support such as forensics collections, intrusion correlation tracking, threat analysis and direct system remediation tasks to on-site responders.
e. Develop and publish malware and forensic analysis guidance and high-quality incident reports to appropriate audiences. (CDRL A002)
f. Provide sound forensic analysis on all devices during malware identification and provide feedback in relation to findings. (CDRL A002)
g. Provide surface and runtime analysis on newly acquired malware to develop new indicators in support of security posture changes to the Enterprise Network.

h. Provide malware analysis to develop incident timelines to include: the dates and times of significant events, command and control domains, and call back addresses; threat objective; and compromised hosts and data. (CDRL A002)
i. Support custom signature and correlation rules creation to enhance Enterprise Network protections.
j. Support the creation of a 'big data' analysis program through the identification of attributes and indications of targeted activity for profile development within the deployed DCOS sensor grid.
k. Analyze Malware to determine its capabilities, intent, indicators and origin.
l. Reverse engineer the sequence of events of a breach or attack.
m. Reverse engineer malware, using Dynamic and Static analysis.
n. Create alerts and identify indicators of compromise to facilitate detection and prevention of similar attacks.
o. Research new attacks and exploits.
p. Identify trends in incidents and malware to DCOS leadership. (CDRL A002)
q. Safeguard evidence, remediate and report incidents in accordance with approved procedures. Document findings; provide reports which incorporate intelligence information provided by the Intelligence branch, historical attack information, as well as current and future (projected/possible) threats targeting the Enterprise Network. (CDRL A002)
r. Provide support required to maintain the Government's CSSP accreditation per the standards set forth in the CSSP program manual, DOD-8530.1-M, (dated 17 Dec 03 or later) to include documentation and technical writing support as needed.

5.2.3.2. Exploit Analysis

The Contractor shall be responsible for providing capabilities necessary to review exploit code, their associated vulnerabilities, discover enterprise security discrepancies, assessing associated risk and assisting in the development of remedial action in coordination with the Mitigation Action Team. This team will conduct a thorough analysis of the capabilities and effects of adversary tactics, techniques, and procedures within the Enterprise Network in order to improve the overall defense posture. This team will also support the discovery of vulnerabilities in the production environment including no-notice external security assessments.

The Contractor shall:
a. Create and maintain the body of documentation that describes the tactics, techniques and procedures that comprise the Enterprise Network Exploit Analyst team (CDRL A002).
b. Personnel supporting this task shall obtain a certification in the Red Team Operations Course (See Paragraph 12.2) to further develop expertise on network attack methods.
c. Prioritize mitigation actions based on assessed risk upon discovery of critical exploits and vulnerabilities within the lab and production environments.
d. Conduct, analyze and review penetration tests and Joint Red Team assessment results to develop recommendations to protect the Enterprise Network. (CDRL A002)
e. Analyze and review application, system, and network security postures across the Enterprise Network in both lab and production environments through active scanning, application-layer protocol fingerprinting or traffic analysis.
f. Evaluate identified targeted environments in the Enterprise Network for compliance with applicable DOD, DON, and other government IT Security Policies (i.e. Secure Technical Implementation Guides)
g. Support the development and implementation of enterprise mitigation actions in response to complex vulnerabilities.
h. Maintain a lab environment with current Enterprise Network and defensive configurations in order to test adversary tactics, techniques, and procedures against a mock Enterprise Network (space, software, hardware and relevant configurations provided by government).
i. Develop the processes and procedures for replaying network attacks/compromises within a lab environment in order to scope the situation and develop recommended mitigation actions. (CDRL A002)
j. Support the creation of a repeatable data analysis process which identifies attributes and indications of targeted activity for profile development within the DCOS sensor grid.
k. Provide support required to maintain the Government's CSSP accreditation per the standards set forth in the CSSP program manual, DOD -8530.1-M, (dated 17 Dec 03 or later) to include documentation and technical writing support as needed. (CDRL A002)

5.3. Sensor Grid Support (SGS)

The Contractor shall be responsible for providing support to the Sensor Grid Support (SGS) team. Activities in support of this task include Host Security, Sensor Management, Signature Management and supporting development roles. The Contractor shall be responsible for the installation, operation, and maintenance of all defensive cyber infrastructures on the Enterprise Network, as well as perform systems integration with Network Operations reporting to support defensive activities.

5.3.1 Host Based Security

The Contractor shall leverage the host protection software directed for use by the Government to review events and logs to detect anomalies. The Contractor shall scan systems for vulnerabilities and indications of compromise. The Contractor shall be responsible for providing reports to the appropriate compliance mandated by parent organizations. The Contractor shall be responsible for overall compliance, identification of anomalies and coordination with Signature Management personnel to develop custom host-based signatures to automate the detection of events of interest.

The Contractor shall:

a. Monitor host-based detection consoles for events of interest on end systems and provide anomaly reports to the DCOS Incident Management.
b. Assess endpoints on the Enterprise Network to meet DOD malware scanning and HBSS compliance requirements.
c. Participate in the planning and implementation of new host based technology on the Enterprise Network.
d. Provide daily reports to DCOS leadership detailing trends in host compliance, anomaly activity and vulnerability statistics. (CDRL A002)
e. Maintain a test environment with all host assessment applications and innovate techniques to detect events of interest across the Enterprise Network.
f. Maintain and ensure DCOS e-Policy Orchestrator servers are configured, analyzed, monitored and adequately patched in accordance with applicable DOD directives.
g. Install, operate, maintain, and troubleshoot HBS agents, modules, extensions, deployment tasks, and tags in order to provide required functionality to defend the Enterprise Network.
h. Support the Host Assessment Team (HAT) on a weekly basis to analyze systems on the Enterprise Network to identify vulnerabilities, anomalous host behavior, compromised network hardware and advanced malware.
i. Provide support required to maintain the Government's CSSP accreditation per the standards set forth in the CSSP program manual, DOD-8530.1-M, (dated 17 Dec 03 or later) to include documentation and technical writing support as needed. (CDRL A002)
j. Maintain compliance with the standards required by DISA Command Cyber Readiness Inspection (CCRI) in accordance with DISA and parent organization guidelines.

5.3.2 Network Sensor Support

The Contractor shall ensure system availability, and conduct system administration, installation, troubleshooting and configuration support for Enterprise Network defense sensors and scanners, including all hardware and software used to conduct CSSP functions throughout the Enterprise Network. The Contractor shall provide 24 x 7 x 365 Network Sensor Support coverage from the primary site in Quantico, VA. Additional on-site support is required at the secondary location in San Diego, CA.

The Contractor shall:

a. Maintain and refine the body of documentation that describes DCOS Network Sensor Support Technicians' tactics, techniques and procedures (CDRL A002).
b. Perform system administration of specialized network defense systems to include installation, configuration, maintenance, backup and restoration.
c. Identify potential conflicts with implementation and integration of specialized network defense systems within the network to protect the overall availability of the Enterprise Network.
d. Maintain a network defense test environment to evaluate new applications, signatures, rules, filters and

configurations of managed network defenses systems.

e. Create, maintain, and refine network traffic flow diagrams for the Enterprise Network reflecting the current state of all security applications. (CDRL A002)
f. Manage user accounts and permissions on Enterprise Network defense sensors and scanners.
g. Provide network defense system implementation, installation and configuration support to Government installations and forces operating in deployed environments.
h. Provide detailed and near real time reporting on the status and availability of network sensors deployed across the Enterprise Network.
i. Conduct life-cycle management on the body of enterprise defensive configurations. Provide quarterly reports on the status of Enterprise defensive configuration life-cycle management to DCOS leadership.
j. Analyze network based events daily to identify large numbers of false positive alerts. Modify host-based signatures to eliminate false-positive alerts. Provide monthly metrics on the number and nature of these tuning efforts to DCOS leadership. Provide SIEM subject matter expertise leveraging McAfee's Nitro Security (or Enterprise Security Manager) toolset for administration, operations, and advanced correlation. (CDRL A002)
l. Analyze SIEM views daily to ensure views support Incident Management analyst detection tasks. Modify SIEM views to eliminate false-positive or unnecessary alerts. Provide monthly metrics on the number and nature of these tuning efforts to DCOS leadership. (CDRL A002)
m. Support the Host Assessment Team (HAT) to analyze systems on the Enterprise Network to identify vulnerabilities, anomalous host behavior, compromised network hardware and advanced malware.
n. Provide support required to maintain the Government's CSSP accreditation per the standards set forth in the CSSP program manual, DOD O-8530.1-M, (dated 17 Dec 03 or later) to include documentation and technical writing support as needed. (CDRL A002)

5.3.3 Signature Management and Development

The Contractor shall be responsible for the continuous development and refinement of signatures, policies, configurations, scripts and indicators used to identify malicious or unauthorized activity via network, host, and scanning based detection on the Enterprise Network. The Contractor shall directly maintain and evolve the Enterprise Network's defense detection strategy to keep pace with emerging threats and adversarial techniques, for both internal and external networks, as well as host based security.

The Contractor shall:

a. Create and maintain and refine the body of documentation that describes DCOS Signature Maintenance and Development tactics, techniques and procedures (CDRL A002).
b. Provide subject matter expertise in creation, editing, and management of signatures, rules and filters for specialized network defense systems including but not limited to network and host-based IDS, IPS, firewall, web application firewall, proxy and SIEM systems.
c. Analyze host and network based events daily to identify large numbers of false positive alerts. Modify host-based signatures to eliminate false-positive alerts. Provide monthly metrics on the number and nature of these tuning efforts to DCOS leadership. (CDRL A002)
d. Coordinate with the DCOS Incident Management Section to manage required changes to the signatures, rules and filters of specialized network defense systems.
e. Identify potential conflicts with implementation and integration of specialized network defense systems within the network to protect the overall availability of the Enterprise Network.
f. Using a government provided facility and government provided hardware, the Contractor shall administer and develop a test environment to evaluate new applications, signatures, rules, filters and configurations of managed network defenses systems.
g. Perform life-cycle configuration management of applications, signatures, rules, filters and configurations of managed network defenses systems.
h. Support enterprise mitigation efforts based on the specific monitoring and filtering capabilities of existing network defense infrastructure.
i. Conduct in-depth traffic analysis of documented covert channels to create tailored response signatures.
j. Provide a visual baseline display of CND events of interest from all applicable data sources, to enable the detection of significant events for the Watch Analysts.

k. Improve SIEM correlation rules employing events from multiple data sources to provide more reliable CND alerts.
l. Maintain a test environment with all DCOS signature-based applications and innovate techniques to detect events of interest in the Enterprise Network.
m. Manage and improve the government's defensive detection strategy through the deployment of new signature policies and robust correlation rules for the SIEM (prioritize the network event view for the Watch Analyst team).
n. Provide Database Administrators and Developers to support enterprise network defense databases and supporting systems, including administer, maintain (backups, STIGs, patches, etc.), and develop and implement custom capabilities in structured query language (SQL), .NET and VB .NET
o. Support the Host Assessment Team (HAT) in a weekly analysis of systems on the Enterprise Network to identify vulnerabilities, anomalous host behavior, compromised network hardware and advanced malware.
p. Provide support required to maintain the Government's CSSP accreditation per the standards set forth in the CSSP program manual, DOD O-8530.1-M, (dated 17 Dec 03 or later) to include documentation and technical writing support as needed. (CDRL A002)

5.4. Information Assurance (Host Assessment)

The Contractor shall perform all functions in executing vulnerability management, to include the operation of the Enterprise Network's Information Assurance Vulnerability Management (IAVM) program for DCOS-maintained systems. The Contractor shall be responsible for DCOS' operation of the IAVM program and shall align with the CJCSM 6510.01B, "Cyber Incident Handling Program," dated 10 July 2012 or later.

The Contractor shall:
a. Perform weekly vulnerability audits, submit Plans of Action and Milestone (POA&M) and assist with patching for all DCOS systems in order to maintain compliance with operational directives. (CDRL A002)
b. Conduct malicious file scanning and report findings monthly for identification of potentially compromised systems. (CDRL A002)
c. Maintain the certification and accreditation documentation (DOD IA Certification and Accreditation Process / Risk Management Framework) for all specialized network defense systems and software used on the Enterprise Network in accordance with applicable DOD policies.
d. Support the Host Based team to identify anomalous network and host activity across the Enterprise Network.

5.5. DCOS Support Operations

5.5.1. Knowledge Management and Portal Administration

The Contractor shall be responsible for knowledge management activities in support of DCOS operations. The Contractor shall develop and refine DCOS standard operating procedures, design and improve information sharing throughout DCOS, and coordinate training/exercise planning for all DCOS personnel (Military, Civilian, and Contractor). The Contractor shall be responsible for continuity of services as data sources evolve to changes in the Government's technical computing environment as well as by mandates from parent organizations.

The Contractor shall:
a. Maintain the body of documentation that describes the tactics, techniques and procedures that comprise the DCOS Knowledge Management team. (CDRL A002)
b. Create, edit, and manage a DCOS collaborative SharePoint site to coordinate operations, documentation, and training.
c. Coordinate schedule and logistics for all DCOS training, exercise, and travel in support of operational requirements.
d. Coordinate and manage internal training calendars via NIPRNETEKO, post and advertise available classes.
e. Advise and assist all personnel with their applicable position training requirements and assist all personnel in registration of training classes via DCOS training calendar and/or through a third-party vendor.

f. Administer all aspects of the DCOS web presence, to include development and refinement of the current SharePoint instances and any future requirements.
g. Maintain format and content for the existing DCOS Training and Exercise Employment Plan (TEEP); Collect internal updates and publish weekly for internal information awareness. (CDRL A002)
h. Maintain the DCOS personnel recall roster and POC databases.
i. Track the DCOS personnel training; collect internal updates and publish weekly for internal awareness. (CDRL A002)
j. Format correspondence, briefs, and operational products per the standards set forth in the Secretary of the Navy Manual (SECNAV-M) 5216.5, "Department of the Navy Correspondence Manual," dated March 2010 or other organizational standard. (CDRL A002)
k. Develop and manage the methods to capture, share, and better utilize DCOS organizational knowledge.

5.5.2. Mitigation Action

The Contractor shall be responsible for providing a capability to develop and execute enterprise remediation measures that reduce the impact of vulnerabilities and mitigate risk to the Enterprise Network. Historically, the network management team processes approximately 2000 intelligence reports and 360 waivers for access to Internet web sites per year. Approximately 1 briefing and 2 reports documenting mitigation actions are developed per week.

The Contractor shall:

a. Create and maintain the body of documentation that describes the tactics, techniques and procedures that comprise the Mitigation Action Team. (CDRL A002)
b. Coordinate and track requirements levied upon the DCOS from external commands / agencies and internal sections to ensure actions are completed as required.
c. Develop and implement enterprise mitigation actions in response to intelligence reports, complex vulnerabilities, threats and risks.
d. Manage, prioritize and resolve all open enterprise mis-configurations, by tasking and supervising actions necessary per DOD policy and IA / CND best practices.
e. Perform trend analysis of all available reporting within the DCOS to include review of open/closed incidents, identified exploits, and scan results. (CDRL A002)
f. Provide reports and briefings documenting mitigation actions in appropriate organizational templates. (CDRL A002)
g. Maintain a historical record detailing existing network boundary policy configurations and network perimeter security compliance. (CDRL A002)
h. Review and recommend updates to network/system configurations in response to changes in the threat environment (identified trends, IA vulnerability alerts / bulletins / technical advisories, known malicious files, zero day exploits, etc.), as appropriate.
i. Develop and maintain usable strategies that leverage existing infrastructure to provide improved defenses to the Enterprise Network.
j. Document and maintain the cross-organizational tactics, techniques, and procedures required to implement these strategies. (CDRL A002)
k. Develop and implement strategies to compress the software vulnerability life-cycle.
l. Identify, monitor, and audit relevant enterprise cyber key terrain to protect the Enterprise Network.
m. Conduct defensive cyber operations planning utilizing the government Process, per the standards set forth in policies that will be provided after award to include documentation and planning support as needed.
n. Provide support required to maintain the Government's CSSP accreditation per the standards set forth in the CSSP program manual, DDOD O-8530.1-M, (dated 17 Dec 03 or later) to include documentation and technical writing support as needed.

5.5.3. Information Assurance Red Team (IART)

The Contractor shall be responsible for providing operational network exploitation and cyber threat emulation testing support towards local area network and wide area network systems and components and shall align with the NIST 800-115 and the CJCSM. The IART conducts approximately 10-15 full scale Red Team operations per year, 20 phishing assessments, and 5 assessments of DCOS Time to Detect and Time to respond metrics. This support consists of the development of custom malware in support of targeted operations that range from two weeks in

duration to operations that last approximately four to six weeks in duration. These operations evaluate and assess the security posture of individual units both in garrison and deployed as well as assessments of the government Enterprise Network. Additionally, the IART participates as opposing forces in approximately 8 DOD cyber exercises per year.

The Contractor shall:

a. Create and maintain the body of documentation that describes Government's Red Team's formal network penetration methodology (CDRL A002).
b. Review and refine methodologies to successfully conduct Red Team operations.
c. Develop plans to successfully conduct network exploitation, penetration testing, cyber threat emulation and Red Team operations (CDRL A002).
d. Conduct no-notice and cooperative Red Team assessments and operations.
e. Develop and submit detailed reports of findings, analysis and recommendations (CDRL A002).
f. Research existing exploit code and/or develop proof-of-concept or exploit code for test and evaluation of mitigations solutions.
g. Develop and maintain custom applications (malware development) to support mission requirements to ensure Command and Control during Red Team operations.
h. Identify potential network and system vulnerabilities and mis-configurations through the use and expert employment of all available Enterprise Network scanning and discovery systems (CDRL A002).
i. Provide the support required maintaining the Government's accreditation per the standards set forth in the CJCSM 6510.03, to include documentation and technical writing support as needed.

5.6. Training

The Government has implemented a workforce training program aligned to the DOD Directive 8570.01-M "Information Assurance Workforce Improvement Program" (dated 10 November 2015 or later). The workforce training program supports adherence to the manual for obtaining appropriate certifications, training and ongoing skills development required of the information assurance workforce. The Contractor is a partner in accomplishing the program's objectives and is responsible for maintaining a qualified workforce and supporting delivery of the training program. The Contractor is expected to identify, develop, and implement additive defensive cyber training that advances the workforce's efficacy beyond initial training requirements. The Contractor shall assist the Government in constantly updating the training standard in order to keep pace with the maturation of defensive cyber operations. In addition, the Contractor may be required to attend cyber-related training events/conferences in support of the cyber defense program.

The Contractor shall:

a. Develop and implement a training plan (CDRL A002) that complies with the requirements of each position as outlined by the training requirements in paragraph 12.2 below (also refer to DOD Directive 8570.01-M "Information Assurance Workforce Improvement Program"). The Training Management Plan shall describe how the Contractor will achieve the DCOS training described in paragraph 12.2 (DCOS Internal Training, DOD 8570 Information Assurance track and DOD 8570 CNDSP track) for each contractor employee. The offeror's plan shall ensure that the three applicable training tracks are met within 180 days of employee hire. The Training Management Plan shall list all current certifications held by key and non-key personnel and articulate how it will maintain a certified workforce through the duration of the TO.

b. Deliver DCOS Internal Training:
    - Provide courseware maintenance and course materials in support of Watch Team, Incident Response, Advanced Incident Handling, Hunt, Malware and Forensics, Exploit Analysis, Host Based Security, Network Sensor Support, Signature Development, Mitigation Action, and Red Team (CDRL A002).
    - Instructors must be actively supporting the task area for which they provide training. Each course is to be taught approximately once a quarter. Provide courseware for associated task and subtask areas (Watch Team, Incident Response, Advanced Incident Handling, Hunt, Malware and Forensics, Exploit Analysis, Host Based Security, Network Sensor Support, Signature Development, Mitigation Action, and Red Team) for all DCOS training.

c. Develop and maintain a Defensive Cyber Operations Training and Readiness (T&R) manual per guidance that will be provided after award (CDRL A002). The objective of a DCOS T&R manual is the generation of operational standards for defensive personnel and the training regimens which accomplish those standards. A final product should provide individual, team, and section standards. As DOD and DCOS training requirements change, the T&R shall be updated accordingly.

d. Develop and implement scenario based training (SBT) for each task requiring training. SBT's, also referred to as Tactical Decision Games (TDG), are collaborative group events intended to evaluate the performance of groups in response to a select problem drawn from common operational events (CDRL A002). The scenarios evaluated should be nested in the Defensive Cyber Operations Training and Readiness (T&R) manual that the Contractor develops. At a minimum, the scenarios should evaluate the team's proficiency of execution for each Tailored Readiness Option, Internal Defensive Measure, and Defensive Counter-Measure. The Contractor shall deliver this training to all personnel in each DCOS section on a quarterly basis.

e. Personnel Training Certification Requirements

5.7. Surge Support

The contractor shall provide a Surge Support Plan (CDRL A002) which identifies its procedures and timelines for providing surge support to the Government. Surge support shall be defined by milestones and last no longer than six months in duration without the approval of the CO. The process for initiating surge support shall be completed on a case-by-case basis, approved by the Government.

The contractor shall maintain a recall roster to facilitate surge support in order to maintain operations during planned or unplanned (emergent) cyber events.

5.7.1. Planned Surge Support

The contractor shall provide a surge capability and support for government Cyber Defense requirements and systems. The contractor shall be prepared to provide staff resource support for unanticipated, as-needed surge support requirements for the following sections: cyber watch, incident response, advanced incident handling, mitigation action, information assurance, signature management and development, network sensor support, host sensor technicians, cyber threat analysis cell, hunt team, red team, database administrators, tool development and deployment, and training on short notice (i.e. few days to a month based on urgency). The general expectation is for the contractor to respond within 10 to 14 days of the surge request.

5.7.2. Emergent Surge Support

The contractor shall provide an emergent surge capability and support for government Cyber Defense requirements and systems. The contractor shall be prepared to provide staff resource support for unanticipated, as-needed surge support requirements for the following sections: cyber watch, incident response, advanced incident handling, mitigation action, information assurance, signature management and development, network sensor support, host sensor technicians, cyber threat analysis cell, hunt team, red team, database administrators, tool development and deployment on short notice (hours). The general expectation is for the contractor to respond immediately to maintain operations.

6. CYBER SECURITY (CS) WORKFORCE

The following CS workforce categories, levels, training, and certifications are required for contractor personnel under this task order:

The Contractor shall ensure that personnel accessing information systems have the proper and current CS certification to perform CS functions identified in the technical requirements section of this PWS in accordance with DOD 8570.01-M, Cyber Security Assurance Workforce Improvement Program. The Contractor shall meet applicable CS certification requirements at time of selection to perform work on this effort, including (a) DOD-approved CS workforce certification appropriate for each specified category and level and (b) appropriate operating

system certification for CST positions as required by DOD 8570.01-M. Contractor personnel who do not have proper and current certifications shall be denied access to DOD information systems for the purpose of performing CS functions.

The contractor shall provide documentation supporting the CS certification status of personnel performing CS functions, reporting current CS certification status and compliance using CDRL Contractor Roster, DI-MGMT-81596 in the format prescribed by the COR (CDRL A004).

CYBERSECURITY COMPLIANCE

Cybersecurity (which replaced the term Information Assurance (IA)) is defined as prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation. Contractor personnel shall perform tasks to ensure Navy applications, systems, and networks satisfy Federal/DoD/DON/Navy cybersecurity requirements.

CYBER IT AND CYBERSECURITY PERSONNEL

(a) The Cyberspace workforce elements addressed include contractors performing functions in designated Cyber IT positions and Cybersecurity positions. In accordance with DFARS Subpart 239.71, DoDD 8140.01, SECNAVINST 5239.20A, and SECNAV M-5239.2, contractor personnel performing cybersecurity functions shall meet all cybersecurity training, certification, and tracking requirements as cited in DoD 8570.01-M prior to accessing DoD information systems. Proposed contractor Cyber IT and cybersecurity personnel shall be appropriately qualified prior to the start of the contract performance period or before assignment to the contract during the course of the performance period.

(b) The contractor shall be responsible for identifying, tracking and reporting cybersecurity personnel, also known as Cybersecurity Workforce (CSWF) and Cyber IT workforce personnel. Although the minimum frequency of reporting is monthly, the task order can require additional updates at any time.

(c) Contractors that access Navy IT shall also follow guidelines and provisions documented in Navy Telecommunications Directive (NTD 10-11) and are required to complete a System Authorization Access Request (SAAR) – Navy form.

When a contractor requires logical access to a government IT system or resource (directly or indirectly), the required CAC will have a Public Key Infrastructure (PKI). A hardware solution and software (e.g., ActiveGold) is required to securely read the card via a personal computer. Pursuant to DoDM 1000.13-M-V1, CAC PKI certificates will be associated with an official government issued e-mail address (e.g. .mil, .gov, .edu). Prior to receipt of a CAC with PKI, contractor personnel shall complete the mandatory Cybersecurity Awareness training and submit a signed System Authorization Access Request Navy (SAAR-N) form to the contract's specified COR. Note: In order for personnel to maintain a CAC with PKI, each contractor employee shall complete annual cybersecurity training. The following guidance for training and form submittal is provided; however, contractors shall seek latest guidance from their appointed company Security Officer and the SSC Pacific Information Assurance Management (IAM) office:

1. For annual DoD Cybersecurity/IA Awareness training, contractors shall use this site: https://twms.nmci.navy.mil/. For those contractors requiring initial training and do not have a CAC, contact the SSC Pacific IAM office at phone number (843)218-6152 or e-mail questions to ssc_lant_iam_office.fcm@navy.mil for additional instructions. Training can be taken at the IAM office or online at http://iase.disa.mil/index2.html.
2. For SAAR-N form, the contractor shall use OPNAV 5239/14 (Rev 9/2011). Contractors can obtain a form from the SSC Pacific IAM office at or from the website: https://navalforms.documentservices.dla.mil/. [insert applicable contract information] Digitally signed forms will be routed to the IAM office via encrypted e-mail to ssclant_it_secmtg@navy.mil.

(d) Contractor personnel with privileged access will be required to acknowledge special responsibilities with a Privileged Access Agreement (PAA) IAW SECNAVINST 5239.20A.

DESIGN, INTEGRATION, CONFIGURATION OR INSTALLATION OF HARDWARE AND SOFTWARE
The contractor shall ensure any equipment/system installed or integrated into Navy platform will meet the cybersecurity requirements as specified under DoDI 8500.01. The contractor shall ensure that any design change, integration change, configuration change, or installation of hardware and software is in accordance with established DoD/DON/Navy cyber directives and does not violate the terms and conditions of the accreditation/authorization issued by the appropriate Accreditation/Authorization official. Contractors that access Navy IT are also required to follow the provisions contained in DON CIO Memorandum: Acceptable Use of Department of the Navy Information Technology (IT) dtd 12 Feb 16. Use of blacklisted software is specifically prohibited and only software that is registered in DON Application and Database Management System (DADMS) and is Functional Area Manager (FAM) approved can be used as documented in para 5.2.2. Procurement and installation of software governed by DON Enterprise License Agreements (ELAs) – Microsoft, Oracle, Cisco, Axway, Symantec, ActivIdentity, VMware, Red Hat, NetApp, and EMC shall be in accordance with DON CIO Policy and DON ELAs awarded.

CYBERSECURITY WORKFORCE (CSWF) REPORT (CDRL A004)
DoD 8570.01-M and DFARS PGI 239.7102-3 have promulgated that contractor personnel shall have documented current cybersecurity certification status within their contract. The contractor shall develop, maintain, and submit a CSWF Report as applicable at the task order level. IAW clause DFARS 252.239-7001, if cybersecurity support is provided, the contractor shall provide a Cybersecurity Workforce (CSWF) list that identifies those individuals who are IA trained and certified. Utilizing the format provided at the task order level, the prime contractor shall be responsible for collecting, integrating, and reporting all subcontractor personnel. See applicable DD Form 1423 for additional reporting details and distribution instructions. Contractor shall verify with the COR or other government representative the proper labor category cybersecurity designation and certification requirements.

INFORMATION TECHNOLOGY (IT) SERVICES REQUIREMENTS
This paragraph only applies to IT contracts. Information Technology (IT) is defined as any equipment or interconnected system(s) or subsystem(s) of equipment that is used in the automatic acquisition, storage, analysis, evaluation, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data of information by the agency. IT includes computers, ancillary equipment, peripherals, input, output, and storage devices necessary for security and surveillance. Electronic and Information technology (EIT) is IT that is used in the creation, conversion, or duplication of data or information. EIT includes: telecommunication products, such as telephones; information kiosks; transaction machines; World Wide Web sites; multimedia (including videotapes); and office equipment, such as copiers and fax machines.

INFORMATION TECHNOLOGY (IT) GENERAL REQUIREMENTS
When applicable, the contractor shall be responsible for the following:
• Ensure that no production systems are operational on any RDT&E network.
• Follow DoDI 8510.01 of 12 Mar 2014 when deploying, integrating, and implementing IT capabilities.
• Migrate all Navy Ashore production systems to the NMCI environment where available.
• Work with government personnel to ensure compliance with all current Navy IT & cybersecurity policies, including those pertaining to Cyber Asset Reduction and Security (CARS).
• Follow SECNAVINST 5239.3B of 17 June 2009 & DoDI 8510.01 of 12 Mar 2014 prior to integration and implementation of IT solutions or systems.
• Register any contractor-owned or contractor-maintained IT systems utilized on contract in the Department of Defense IT Portfolio Registry (DITPR)-DON.
• Only perform work specified within the limitations of the task order.

ACQUISITION OF COMMERCIAL SOFTWARE PRODUCTS, HARDWARE, AND RELATED SERVICES
This paragraph only applies to the purchasing/hosting of commercial software. Contractors recommending or purchasing commercial software products, hardware, and related services supporting Navy programs and projects shall ensure they recommend or procure items from approved sources in accordance with the latest DoN and DoD policies.

DON ENTERPRISE LICENSING AGREEMENT/DOD ENTERPRISE SOFTWARE INITIATIVE PROGRAM

Pursuant to DoN Memorandum – Mandatory use of DoN Enterprise Licensing Agreement (ELA) dtd 22 Feb 12, contractors that are authorized to use Government supply sources per FAR 51.101 shall verify if the product is attainable through DoN ELAs and if so, procure that item in accordance with appropriate ELA procedures. If an item is not attainable through the DoN ELA program, contractors shall then utilize DoD Enterprise Software Initiative (ESI) program (see DFARS 208.74) and government-wide SmartBuy program (see DoD memo dtd 22 Dec 05). The contractor shall ensure any items purchased outside these programs have the required approved waivers as applicable to the program. Software requirements will be specified at the task order level.

DON APPLICATION AND DATABASE MANAGEMENT SYSTEM (DADMS)

The contractor shall ensure that no Functional Area Manager (FAM) disapproved applications are integrated, installed or operational on Navy networks. The contractor shall ensure that all databases that use database management systems (DBMS) designed, implemented, and/or hosted on servers and/or mainframes supporting Navy applications and systems be registered in DoN Application and Database Management System (DADMS) and are FAM approved. All integrated, installed, or operational applications hosted on Navy networks must also be registered in DADMS and approved by the FAM. No operational systems or applications will be integrated, installed, or operational on the RDT&E network.

INFORMATION SECURITY

Pursuant to DoDM 5200.01, the contractor shall provide adequate security for all unclassified DoD information passing through non-DoD information system including all subcontractor information systems utilized on contract. The contractor shall disseminate unclassified DoD information within the scope of assigned duties and with a clear expectation that confidentiality is preserved. Examples of such information include the following: non-public information provided to the contractor, information developed during the course of the contract, and privileged contract information (e.g., program schedules, contract-related tracking).

IT POSITION CATEGORIES

Pursuant to DoDI 8500.01, DoD 8570.01-M, SECNAVINST 5510.30, SECNAV M-5239.2, and applicable to unclassified DoD information systems, a designator is assigned to certain individuals that indicates the level of IT access required to execute the responsibilities of the position based on the potential for an individual assigned to the position to adversely impact DoD missions or functions. As defined in DoD 5200.2-R, SECNAVINST 5510.30 and SECNAV M-5510.30, three basic DoN IT levels/Position categories exist:

- IT-I (Privileged access)
- IT-II (Limited Privileged, sensitive information)

Note: The term IT Position is synonymous with the older term Automated Data Processing (ADP) Position (as used in DoD 5200.2-R, Appendix 10). Investigative requirements for each category vary, depending on the role and whether the individual is a U.S. civilian contractor or a foreign national. The Contractor PM shall assist the Government Project Manager or COR in determining the appropriate IT Position Category assignment for all contractor personnel. All required Single-Scope Background Investigation (SSBI)/Tier 5, SSBI Periodic Reinvestigation (SSBI-PR)/Tier 5R, and National Agency Check (NAC)/Tier 3R adjudication will be performed Pursuant to DoDI 8500.01 and SECNAVINST 5510.30. Requests for investigation of contractor personnel for fitness determinations or IT eligibility without classified access are submitted by SPAWAR/SSC Atlantic/SSC Pacific Security Office, processed by the OPM, and adjudicated by DOD CAF. IT Position Categories are determined based on the following criteria:

> IT-I Level (Privileged) - Positions in which the incumbent is responsible for the planning, direction, and implementation of a computer security program; major responsibility for the direction, planning and design of a computer system, including the hardware and software; or, can access a system during the operation or maintenance in such a way, and with a relatively high risk for causing grave damage, or realize a significant personal gain. Personnel whose duties meet the criteria for IT-I Position designation require a favorably adjudication of Single Scope Background Investigation (SSBI)/Tier 5 or SSBI-PR/Tier 5R. The SSBI/Tier 5 or SSBI-PR/Tier 5R is updated a minimum of every 5 years. Assignment to designated IT-I positions requires U.S. citizenship unless a waiver request is approved by CNO.

IT-II Level (Limited Privileged) - Positions in which the incumbent is responsible for the-direction, planning, design, operation, or maintenance of a computer system, and whose work is technically reviewed by a higher authority at the IT-II Position level to insure the integrity of the system. Personnel whose duties meet the criteria for an IT-II Position require a favorably adjudication of a Position of Trust National Agency Check with Law and Credit (PT/NACLC)/Tier 3R. Assignment to designated IT-II positions requires U.S. citizenship unless a waiver request is approved by CNO.

IT-III Level (Non-privileged) - All other positions involved in computer activities. Incumbent in this position has non-privileged access to one or more DoD information systems/applications or database to which they are authorized access. Personnel whose duties meet the criteria for an IT-III Position designation require a favorably adjudication of a Position of Trust National Agency Check with Written Inquiries (PT/NACI).

7. DATA DELIVERABLES

Data deliverables shall be as specified in the attached CDRL.

8. TRAVEL

Contractor costs for travel will be reimbursed at the limits set in the following regulations (see FAR 31.205-46):

a. Joint Travel Regulation (JTR) for travel in the contiguous U.S.
b. Federal Travel Regulation (FTR) Volume 2, Department of Defense (DOD) Civilian Personnel, Appendix A - prescribed by the DOD, for travel in Alaska, Hawaii, and outlying areas of the U.S.
c. Department of State Standardized Regulations (DSSR) (Government Civilians, Foreign Areas), Section 925, "Maximum Travel Per Diem Allowances for Foreign Areas" - prescribed by the Department of State, for travel in areas not covered in the FTR or JTR.

The Contractor may invoice monthly on the basis of cost incurred for cost of travel comparable with the JTR/FTR/DSSR. The invoice shall include the period of performance covered by the invoice, the CLIN number, task area, and title. Separate worksheets, in MS Excel format, shall be submitted for travel (CDRL A001).

All cost presentations provided by the Contractor shall also include Overhead charges and General and Administrative charges in accordance with the Contractor's DCAA cost disclosure statement.

The table below serves solely as an estimate of anticipated travel. Successful awardee is authorized to travel to locations not listed in the table below, provided that the travel is conducted in accordance with JTR Appendix G: Reimbursable Expenses on Official Travel. All travel requests shall be approved by the appointed Contracting Officer Representative (COR).

The following travel is estimated for the performance of the requirements of this PWS:

CLIN	# Trips	# of Travelers	# Days	From (Location)	To (Location)
Base	95	2	4	CONUS	GLOBAL
Option 1	95	2	4	CONUS	GLOBAL
Option 2	95	2	4	CONUS	GLOBAL
Option 3	95	2	4	CONUS	GLOBAL
Option 4	95	2	4	CONUS	GLOBAL

All work is required to be performed onsite at the Government locations specified. The primary site for this work will be on-site in Quantico, VA. The secondary site for this work will be performed at San Diego, CA. During the duration of this task order, the secondary site is anticipated to move to Kansas City, MO, at which time the Government will provide the Contractor with specific relocation requirements.

During contingency operations, the Contractor may be required to temporarily relocate personnel from the primary or secondary sites.

D&CI and SGS personnel will be required to travel approximately two people per month to the CONUS locations, though other locations may necessitate on-site support, in support of on-site incidents response actions or infrastructure upgrades/installations.

Contractor personnel must adhere to all current DoD, SECNAV, OPNAV, and SSC Pacific instructions related to foreign travel.

CONTRACTOR NOTIFICATION – AWARENESS OF EXPECTATIONS

Contractor personnel are reminded of their obligation to safeguard the vital relationship our Nation has with Foreign Countries. This includes personal conduct while performing under the contract and on one's personal time because, at all times, you are viewed by our partners as a representative of the United States, our Navy, and SPAWAR. Therefore, professional, courteous, and culturally aware conduct is necessary at all times. Inappropriate conduct, and especially intoxication and criminal behaviors, will not be tolerated. An all too common nexus for personnel misconduct while on travel is irresponsible consumption of alcohol. Intoxication increases your vulnerability to crime, injury, arrest, terrorism and espionage.

While traveling on official business, representing and performing in support of SPAWAR's mission, all personnel, including military, civilian and contractors, are expected to act in a professional and responsible manner. In order to promote effective relationships with business partners and allied nations, it is incumbent on contractor personnel to follow local laws and employ courteous and culturally aware behavior. Inappropriate conduct may jeopardize important relationships for the United States Navy, SPAWAR, SSC Pacific and SSC Atlantic, and will not be tolerated.
In all cases, contractors are reminded of their responsibilities under FAR 52.203-13, Contractor Code of Business Ethics and Conduct. The clause requires the contractor to:

- Have a written code of business ethics and conduct;
- Make a copy of the code available to each employee;
- Exercise due diligence to prevent and detect criminal conduct;
- Promote an organizational culture that encourages ethical conduct and a commitment to compliance with the law.

The clause also requires contractors to timely disclose, in writing, to the agency Office of the Inspector General (OIG), with a copy to the Contracting Officer, whenever, in connection with the award, performance, or closeout of this contract or any subcontract thereunder, the contractor has credible evidence that a principal, employee, agent, or subcontractor of the contractor has committed—

- A violation of Federal criminal law involving fraud, conflict of interest, bribery, or gratuity violations found in Title 18 of the United States Code; or
- A violation of the civil False Claims Act (31 U.S.C. 3729-3733).

9. PROPERTY REQUIREMENTS

No GFP is anticipated.

Government furnished facilities or workspace will be provided at all required locations as a matter of routine. The Government shall provide, manage and hold custody of facilities, office furnishings, and equipment (hardware & software) used by the Contractor in the performance of work under this Contract. The Government will provide the support staff with the workspaces, desks, telephones, ADP equipment, and software required to perform Contract tasks when and where necessary. The Contractor shall require all personnel to keep the spaces, furnishings and equipment provided for their use in a manner consistent with government standards for fire prevention, health and safety; and takes proper care of all Government property in their possession.

Upon completion or termination of this Contract, any Government furnished equipment, property, or items provided to the Contractor shall be returned to the Government.

10. SECURITY

10.1 Security

The work performed by the Contractor will include access to unclassified and up to Top Secret/Sensitive Compartmented Information (SCI) data, information, and spaces. The contractor will be required to provide individuals with security clearances at the appropriate classification levels. The Contractor will be required to attend meetings classified up to Top Secret/SCI. The Contractor will require access to Communications Security (COMSEC) and the Secure Internet Protocol Router Network (SIPRNet)/Joint Worldwide Intelligence Communications System (JWICS).

Contractor personnel assigned to this effort who require access to SCI data and spaces must possess a current SSBI with ICD 704 eligibility (which replaced DCID 6/4 eligibility).

Although there is no requirement for the contractor to access NATO on this contract per Naval Intelligence Security Policy Directive 17-008 those contractors that have SCI access and those cleared SCI with JWICS or SIPRnet accounts shall be North Atlantic Treaty Organization (NATO) read-on and complete the derivative classification training prior to being granted access to JWICS/SIPRnet; training is provided by the facility security officer. Specific requirements provided in the Department of Defense Contract Security Classification Specification, DD Form 254.

If foreign travel is required, all outgoing Country/Theater clearance message requests shall be submitted to the SSC PACIFIC foreign travel team for action. A Request for Foreign Travel form shall be submitted for each traveler, in advance of the travel, to initiate the release of a clearance message at least 40 days in advance of departure. Each Traveler must also submit a Personal Protection Plan and have a Level 1 Antiterrorism/Force Protection briefing within one year of departure and a country specific briefing within 90 days of departure.

As required by National Industrial Security Program Operating Manual (NISPOM) Chapter 1, Section 3, contractors are required to report certain events that have an impact on: 1) the status of the facility clearance (FCL); 2) the status of an employee's personnel clearance (PCL); 3) the proper safeguarding of classified information; 4) or an indication that classified information has been lost or compromised. Contractors working under SSC Pacific contracts will ensure information pertaining to assigned contractor personnel are reported to the Contracting Officer Representative (COR)/Technical Point of Contact (TPOC), the Contracting Specialist, and the Security's COR in addition to notifying appropriate agencies such as Cognizant Security Agency (CSA), Cognizant Security Office (CSO), or Department Of Defense Central Adjudication Facility (DOD-CAF) when that information relates to the denial, suspension, or revocation of a security clearance of any assigned personnel; any adverse information on an assigned employee's continued suitability for continued access to classified access; any instance of loss or compromise, or suspected loss or compromise, of classified information; actual, probable or possible espionage, sabotage, or subversive information; or any other circumstances of a security nature that would affect the contractor's operation while working under SSC Pacific contracts.

If foreign travel is required, all outgoing Country/Theater clearance message requests shall be submitted to Commanding Officer, Attn: Foreign Travel Team, Space and Naval Warfare Systems Center Pacific, 53560 Hull Street, Building 27, 2nd Floor -Room 206, San Diego, CA 92152 for action. A Request for Foreign Travel form shall be submitted for each traveler, in advance of the travel, to initiate the release of a clearance message at least 30 days in advance of departure. Each Traveler must also submit a Personal Protection Plan and have a Level 1 Antiterrorism/Force Protection briefing within one year of departure and a country specific briefing within 90 days of departure. Anti-Terrorism/Force Protection (AT/FP) briefings are required for all personnel (Military, DOD Civilian, and contractor) per OPNAVINST F3300.53C. Contractor employees must receive the AT/FP briefing annually. The briefing is available at Joint Knowledge Online (JKO): https://jkodirect.jten.mil (prefix): course number: US007; title: Level 1 Anti-terrorism Awareness Training, if experiencing problems accessing this website contact ssc_fortrav@navy.mil. Forward a copy of the training certificate to the previous email address or fax to

(619) 553-6863. Sere 100.2 Level A code of conduct training is also required prior to OCONUS travel for all personnel. Sere 100.2 Level A training can be accessed at http://jko.jfcom.mil (recommended), https://jkodirect.jten.mil/atlas2/faces/page/login/login.seam, and recommend course: prefix: J3T: course #: A-US1329, for civilian, military, and contractors. Personnel utilizing this site must have a CAC. Specialized training for specific locations, such as SOUTHCOM human rights, or U.S. forces Korea entry training, may also be required; SSC Pacific security personnel will inform you if there are additional training requirements. Finally, EUCOM has mandated that all personnel going on official travel to the EUCOM AOR must now register with the Smart Traveler Enrollment Program (STEP). When you sign up, you will automatically receive the most current information the State Department compiles about your destination country. You will also receive updates, including Travel Warnings and Travel Alerts. Sign up is one-time only, after you have established your STEP account, you can easily add official or personal travel to anywhere in the world, not just EUCOM.
http://travel.state.gov/content/passports/en/go/step.html.

Applicable documents are as follows OPNAVINST F3300.53C (Series), Navy Antiterrorism Program SECNAV Manual 5510.30 (Series), Department of Navy Personnel Security Program, SECNAV Manual 5510.36 (Series), Department of Navy Information Security Program, DOD 5200.01 Volumes 1 through 4 (Series), DOD Security Program, and DOD 5220.22-M (Series), National Industrial Security Program Operating Manual (NISPOM).

10.2 Operations Security (OPSEC)

OPSEC is a five step analytical process (identify critical information; analyze the threat; analyze vulnerabilities; assess risk; develop countermeasures) that is used as a means to identify, control, and protect unclassified and unclassified sensitive information associated with U.S. national security related programs and activities. All personnel working under this task will at some time handle, produce or process Critical Information or Critical Program Information, and therefore all Contractor personnel must practice OPSEC. All work is to be performed in accordance with DoD OPSEC requirements, and in accordance with the OPSEC attachment to the DD254.

Applicable documents are as follows, National Security Decision Directive 298 (Series), National Operations Security Program (NSDD) 298, DOD 5205.02-M, DOD Operations Security (OPSEC) Program, OPNAVINST 3432.1A, DON Operations Security, and SPAWARINST 3432.1A, Operations Security Policy.

11. PERFORMANCE REQUIREMENTS SUMMARY

11.1. Performance Requirement. The contractor shall provide services and deliverables in accordance with this PWS and in accordance with the attached task order Contract Data Requirements List (CDRL) items.

11.2. Performance Standard. The contractor's performance shall meet all of the requirements of this PWS and comply with all applicable guidance, directives, and standards. The contractor shall deliver all task order data items in accordance with the authorities, content, format, media, marking, applications, quantities, frequency and submission date, delivery method, addressee, and DD250 requirements specified in the CDRL for each data item.

11.3. Acceptable Quality Level. The effectiveness of the contractor's deliverables and services will be measured for 100% compliance with all PWS and CDRL requirements. The Government will evaluate (1) the quality of services and deliverables in terms of the contractor's compliance with the performance standard, (2) the contractors' timeliness with respect to task order, milestones, and delivery schedules, (3) the contractor's cost control in terms of effectiveness in forecasting, managing, and controlling cost, and (4) the contractor's business relations in terms of timeliness, completeness, quality of problem identification and corrective action, and reasonable and cooperative behavior.

11.4. Hours of Operation and Coverage

Hours of Operation	Shift 1	Shift 2
Standard Hours (Primary Site)	0700-1530 M-F	1500-2330 M-F
Alternate Work Schedule (Primary Site)	0700-1900 S/M/T/Alt Wed 0700-1900 Alt Wed/Th/F/S	1900-0700 S/M/T/Alt Wed 1900-0700 Alt Wed/Th/F/S
Standard Hours (Secondary Site)	0800-1630 M-F	Fail Over/ Emergency

The alternate work schedule referenced above are the shifts required of personnel designated to support 24x7 operations. Personnel supporting 24x7 operations will be required to work under the Alternate Work Schedule. The Alternate Work Schedule supports a rotational 12 hour shift consisting of a three and four day work week within a 2 week cycle.

During federal holidays, times of inclement weather (where hazardous conditions exist between the work site and local community), and other contingency events, The Contractor shall ensure the minimum staffing required to maintain operational effectiveness is met in the Incident Management and Sensor Grid Support functions.

12. OTHER

12.1. Key Personnel

The following are the minimum personnel who shall be designated as "Key Personnel" in accordance with the Key Personnel clause. The Government does not intend to dictate the composition of the ideal team to perform this TO. The threshold for key personnel is one person per role listed below:

a. Program Manager (PM)
b. Discovery & Counter-Infiltration (D&CI) Technical Lead
c. Sensor Grid Support Technical Lead
d. Security Information and Event Manager Subject Matter Expert
e. Red Team Developer Subject Matter Expert
f. Exploit Analysis Cell Subject Matter Expert

12.1.1. Program Manager

It is required that the PM has the following qualifications:

a. Active PMI PMP or DAWIA Level III
b. Bachelor's Degree in Computer Science or related IT field
c. At least five years of experience managing a program of similar in size and scope to that outlined in this PWS.
d. At least ten years of experience supporting a program in a DOD Computing Environment, Network Environment, and enclave environment.
e. Security clearance that meets DD-254 requirements (Section J - Attachment 2)
f. Possess IAT Level II or greater
g. Management experience in an enterprise-level (minimum of 50k users) Computer Network Defense (CND) environment.

12.1.2. D&CI Technical Lead

It is required that the D&CI Technical Lead has the following qualifications:

a. At least five years of demonstrated experience with CND tools, tactics, and techniques in a computer network defense environment.
b. At least five years of experience managing personnel in an information assurance environment.

c. Security clearance that meets DD-254 requirements (Section J - Attachment 2)
d. Possess CNDSP Analyst certification
e. Possess IAT Level III certification
f. Experience handling national state level intrusions.

12.1.3. Sensor Grid Support Technical Lead

It is required that the Sensor Grid Support Technical Lead has the following qualifications:
a. At least five years of demonstrated experience in supporting CND and/or network systems and technology.
b. At least five years of experience managing personnel in an information assurance environment.
c. Security clearance that meets DD-254 requirements (Section J - Attachment 2)
d. Possess CNDSP Infrastructure Support certification
e. Possess IAT Level III certification
f. Experience leading operations and maintenance support for an enterprise-level (minimum of 50k users) sensor grid.

12.1.4. Security Information and Event Manager Subject Matter Expert

It is required that the Security Information and Event Manager Subject Matter Expert has the following qualifications:
a. Experience managing an enterprise-grade Security Information and Event Management toolset, including maintenance, cyber analytics and correlation use cases.
b. At least five years overall experience with CND and cyber security tools
c. Security clearance that meets DD-254 requirements (Section J - Attachment 2)
d. Experience leveraging network and host based sensors and other cybersecurity tools to enhance the detection of adversary activity.
e. Possess IAT Level II certification or greater

12.1.5. Red Team Developer Subject Matter Expert

It is required that the Red Team Developer have the following qualifications:
a. At least five years of experience performing various assessments (penetrations tests of systems and networks within a DOD Network Environment of enclave.
b. At least five years of experience developing exploit code for network and system penetration testing.
c. At least five years of experience developing and maintaining custom applications that exploit known system vulnerabilities or system mis-configurations to gain system command and control during red team operations.
d. Security clearance that meets DD-254 requirements (Section J - Attachment 2)
e. Experience developing undetected malware for use in red team assessments against enterprise-level networks.
f. Possess IAT Level III certification

12.1.6. Exploit Analysis Subject Matter Expert

It is required that the Exploit Analysis Subject Matter Expert have the following qualifications:
a. At least five years of experience performing various assessments (penetrations tests of systems and networks within a DOD Network Environment of enclave.
b. At least five years of experience developing exploit code for network and system penetration testing.
c. At least five years of experience performing penetration testing of web applications
d. At least five years of experience developing specialized applications for the assessment and security testing of web applications.
e. At least five years of experience developing and maintaining custom applications that exploit known system vulnerabilities or system mis-configurations to configurations to gain system command and control during red team operations.

f. Knowledge DOD security controls to include DISA Secure Technical Implementation Guidelines (STIG) and the DOD IA Certification and Accreditation Process and Risk Management Framework (RMF).
g. Security clearance that meets DD-254 requirements (Section J - Attachment 2)
h. Possess IAT Level III certification

12.2. Subject Matter Experts (Non-Key Personnel).

12.2.1. Data Science Subject Matter Expert.

It is required that the Data Science Subject Matter Expert have the following minimum qualifications. The Government reserves the right to review compliance with the minimum Data Science Subject Matter Expert qualifications, in accordance with this PWS, after task order award.

a. At least one year of experience in the cybersecurity field.
b. A Bachelor's Degree in computer science, information technology, cybersecurity, or related field.
c. Successful completion of college-level courses in statistics to include statistical regression.
d. At least two years of experience with data science tools including Elastic Search, Logstash, Kibana, Hadoop, NOSQL, etc.
e. At least two years of experience utilizing the Python scripting language to conduct data analysis.
f. At least two years of experience working with large data-sets to extract actionable insights.
g. Security clearance that meets DD-254 requirements (Section J - Attachment 2)
h. Possess IAT Level II certification

12.3. General Personnel Requirements

The DOD 8570.01-M "Information Assurance Workforce Improvement Program" (dated 24 Jan 2012 or later) established the guidance for personnel requirements conducting Information Assurance (IA) functions. The Government has established training certification requirements for all personnel (key and non-key) supporting this contract. The Contractor must be compliant with the training certification requirements DOD 8570 IA Category and CND-SP Specialty) at the start of the task order or employee hire. The applicable courses and certifications for all personnel supporting this contract are outlined in the table below.

Personnel Training Certification Requirements:

DISCOVERY AND COUNTER-INFILTRATION (D&CI)	DCOS INTERNAL TRAINING	DOD 8570 IA TRACK	DOD 8570 CNDSP TRACK
D&CI TECHNICAL LEAD	WA, HCI AND IR COURSES	IAT LVL 3	CND ANALYST
CYBER WATCH/INCIDENT RESPONSE	WA, HCI AND IR COURSES	IAT LVL 2	CND INCIDENT RESPONDER
ADVANCED INCIDENT HANDLING	IS, HCI AND IR COURSES	IAT LVL 3	CND AUDITOR
MALWARE AND FORENSICS EXPLOIT ANALYST	WA, HCI AND IR COURSES WA, IR, HCI, AND ALL SGS COURSES	IAT LVL 3 IAT LVL 3	CND INCIDENT RESPONDER CND AUDITOR
HUNT TECH	WA, IR, RED TEAM LEVEL I & II	IAT LVL 3	CND AUDITOR
DATA SCIENCE SUBJECT MATTER EXPERT	WA, HCI, AND IR COURSES	IAT LVL 2	CND ANALYST
SENSOR GRID SUPPORT (SGS)	**DCOS INTERNAL TRAINING**	**DOD 8570 IA TRACK**	**DOD 8570 CNDSP TRACK**
SGSTECHNICAL LEAD	WA, HCI ALL IS	IAT LVL 3	CND INFRASTRUCTURE SUPPORT

NETWORK SENSOR SUPPORT	WA, HCI AND SGS COURSES	IAT LVL 2	CND INFRASTRUCTURE SUPPORT
SIGNATURE MANAGEMENT	WA, HCI, IR AND ALL IS COURSES	IAT LVL 3	CND ANALYST
DATABASE ADMINISTRATOR	WA, HCI AND ALL IS COURSES	IAT LVL 2	CND INFRASTRUCTURE SUPPORT
DEVELOPER	WA, HCI AND ALL IS COURSES	IAT LVL 2	CND INFRASTRUCTURE SUPPORT
HOST-BASED SENSOR TECH	WA, HCI, IR, AND ALL SGS COURSES	IAT LVL 2	CND INFRASTRUCTURE SUPPORT
DCOS SUPPORT OPERATIONS	**DCOS INTERNAL TRAINING**	**DOD 8570 IA TRACK**	**DOD 8570 CNDSPTRACK**
MITIGATION ACTION TEAM	WA, HCI AND IS COURSES	IAT LVL 2	CND AUDITOR
KNOWLEDGE MANAGEMENT TEAM	WA AND HCI COURSES	Not Required	Not Required
PORTAL ADMIN	WA AND HCI COURSES	Not Required	Not Required
RED TEAM DEVELOPER	WA, HCI AND IS COURSES	IAT LVL 2	CND IASAE

In accordance with DFARS clause 252.239-7001 and Procedures, Guidance and Information 239.7102, The Contractor shall submit proof of certifications attained for both key and non-key personnel to demonstrate compliance upon request from the Government.

12.4. Enterprise-Wide Contract Management Application (ECMRA).

The contractor shall report ALL contractor labor hours (including subcontractor labor hours) required for performance of services provided under this contract for the SSC Pacific via a secure data collection site. Contracted services excluded from reporting are based on Product Service Codes (PSCs). The excluded PSCs are:

a. W, Lease/Rental of Equipment;
b. X, Lease/Rental of Facilities;
c. Y, Construction of Structures and Facilities;
d. D, Automatic Data Processing and Telecommunications, IT and Telecom-Telecommunications Transmission (D304) and Internet (D322) ONLY;
e. S, Utilities ONLY;
f. V, Freight and Shipping ONLY.

The contractor is required to completely fill in all required data fields using the following web address: https://www.ecmra.mil/.

Reporting inputs will be for the labor executed during the period of performance during each Government fiscal year (FY), which runs October 1 through September 30. While inputs may be reported any time during the FY, all data shall be reported no later than October 31 of each calendar year. Contractors may direct questions to the help desk at: https://www.ecmra.mil/.

For the purposes of CMRA reporting, the Federal Supply Code/Product Service Code applicable to the contract is J070.

(End of PWS)